Die Hacker aus dem Auto aussperren

Konnektivität. Mit Cyberangriffen können vernetzte Pkw ferngesteuert und so Verkehrsunfälle verursacht werden. Ein neues Werkzeug soll Schwachstellen im System schon im Vorfeld erkennen

iNNOVATiON! FORSCHUNGS-MONTAG
KURIER-SERIE

VON **ANDREEA IOSA**

BLUE PLANET STUDIO/ISTOCKPHOTO

Der Straßenverkehr ist ruhig und angenehm. Doch plötzlich macht das Auto wegen eines Rehs auf der Fahrbahn eine Notbremsung. Gleichzeitig leitet es ein Signal an die nachfolgenden Fahrzeuge, sodass deren intelligentes Bremssystem ebenfalls rechtzeitig reagiert. Alle Beteiligten bleiben unversehrt – die Autofahrt kann rasch wieder fortgesetzt werden. Verkehrsszenarien mit vernetzten Autos können aber auch anders aussehen *(siehe unten)*: Greifen Hacker etwa auf intelligente Fahrzeugsysteme zu, können sie die Kontrolle über Türverriegelung, Bremsen, Beschleunigung und mehr erlangen. Wird von der Ferne etwa eine Vollbremsung auf der Autobahn getätigt, ist eine Massenkarambolage vorprogrammiert. Obwohl vernetzte Autos mehr Sicherheit im Verkehr bieten sollen, indem sie mit anderen Fahrzeugen, Online-Diensten und der Infrastruktur kommunizieren, bringen sie also gleichzeitig auch Gefahren mit sich. Und die könnten in Zukunft zu einem massiven Problem werden. Denn laut einer Studie von Juniper Research könnten im Jahr 2023 weltweit schon 780 Millionen Fahrzeuge vernetzt sein.

Neues Werkzeug

Um derartige Bedrohungen ausschließen zu können, müssen Hersteller bald schon vom Entwicklungsbeginn an eine Risikobeurteilung durchführen. „2022 tritt eine neue Regulierung in Kraft: Wer einen neuen Typ zulassen will, muss die UN ECE-Richtlinien bei der Entwicklung berücksichtigen und eine Cybersecurity-Behandlung nachweisen“, sagt Willibald Krenn vom AIT Austrian Institute of Technology dem KURIER. Um diese Analyse so automatisiert und einfach wie möglich zu machen, hat das AIT gemeinsam mit der Softwarefirma LieberLieber das Werkzeug „Threatget“ entwickelt. Wird ein Fahrzeug entworfen, kann man mit diesem Tool festlegen, welche Sicherheitseigenschaften einzelne Komponenten haben sollen.

Was das Werkzeug dafür in erster Linie braucht, ist Information über bereits bestehende bekannte Schwachstellen. „Wir haben dafür eine Bedrohungsdatenbank erstellt, die von uns gewartet und aktualisiert wird“, sagt Krenn. Aber auch Kunden können die Datenbank permanent erweitern.

Verschlüsselung

Basierend auf diesem Wissensschatz könne man ein System modellieren, indem Einzelkomponenten wie Sensoren oder Steuergeräte, die auch in dieser Datenbank vorhanden sind, auf einer Arbeitsfläche verknüpft werden. „Zum Beispiel kann ich sagen, dass die ECU (Electronic Control Unit bzw. Steuergerät) mit dem Sensor verbunden ist, indem ich die Komponenten auf meine Arbeitsfläche ‚ziehe‘ und danach miteinander verknüpfe. So baue ich ein Modell des Gesamtsystems auf“, sagt der Fachmann und ergänzt: „Ich überlege mir also schon hier, was mit wem spricht und welche Sicherheitseinstellungen es braucht.“ Der Anwender könne unter anderem auch festlegen, dass die Verbindung von der ECU zum anderen Element verschlüsselt ist.

Das Tool führt in Folge die Analyse systematisch durch und geht alle Modelle sowie die gesamte Bedrohungsdatenbank durch. Pro Bedrohung spuckt es schließlich einen Eintrag in einer Liste aus – auch gibt das Werkzeug eine grobe Einschätzung dazu. „Der Nutzer schaut sich jede gefundene Bedrohung an und ob die Einstufung des Risikos passt. Am Ende des Ganzen kann er das Ergebnis mit diversen anderen Tools verbinden und sich auch einen Bericht ausgeben lassen, der für Nachweise verwendet werden kann“, sagt der AIT-Experte.

Periodische Analyse

Der große Vorteil dieser Innovation bestehe laut Krenn nicht nur darin, dass die gesamte Bedrohungsdatenbank mit dem Modell abgeglichen werde – das Werkzeug könne zudem auch dann weiterverwendet werden, wenn ein Auto länger am Markt ist. „Ich muss nämlich periodisch untersuchen, ob das Design noch sicher ist. Dafür kann ich das Modell einfach wieder hineinladen und mit der inzwischen aktualisierten Datenbank wieder abgleichen. Ergibt sich ein neues Risiko, kann ich zielgerichtet daran arbeiten“, erzählt er. Experten würden ihm zufolge durch Threatget keinesfalls ersetzt – mit dem System seien aber mehr und effizientere Analysen möglich.

Künstliche Intelligenz

Eine kommerzielle Variante mit der Basisfunktionalität ist laut dem Fachmann bereits am Markt und in Anwendung. Der Automotive-Spezialist msg Plaut Austria hat das System etwa in Projekten mit Fahrzeugzulieferern eingesetzt. „An gewissen Forschungsaspekten arbeiten wir weiter. Zum Beispiel arbeiten wir daran, mit auf künstliche Intelligenz (KI) basierten Methoden das Internet abzusuchen und neue Bedrohungen automatisch herauszufiltern“, sagt Krenn. Auch hinsichtlich der Empfehlungen und Lösungsvorschläge bei potenziellen Risiken, die das System ausspuckt, werde noch geforscht. „Für gewisse Bedrohungen sind in der Bedrohungsdatenbank aber schon Hinweise hinterlegt,“ betont der Fachmann.

Generell sei Threatget für alle Dienstleister aus der Automobilindustrie gedacht, etwa für Erstausrüster oder für jene im Bereich Systemdesign. „Prinzipiell können alle, die Security bei ihrem Design brauchen, von Threatget Gebrauch machen. Generell bemühen wir uns jetzt um die Automobil-Industrie, weil die neuen Standards anstehen. Die Idee ist aber auch in anderen Sektoren einsetzbar.“

Wie vernetzte Fahrzeuge bereits ferngesteuert wurden

Angreifer können über Schwachstellen Autos abbremsen

Cyberattacken. Vernetzte Autos sollen die Sicherheit auf den Straßen erhöhen. Allerdings lassen sich die Fahrzeuge auch von Hackern aus der Ferne kapern und kontrollieren. Forscher haben im vergangenen Jahr in 40 Motorsteuerungseinheiten von 10 Herstellern bzw. Zulieferern mehr als 300 Schwachstellen entdeckt.

Autodiebstahl

Laut dem AIT Austrian Institute of Technology wurden im vergangenen Jahr 19 Schwachstellen in einem Mercedes-Benz-E-Klasse-Wagen entdeckt. Die haben Hackern Zugang zu den Türen und Kontrolle über den Motor gegeben.

In Indien wiederum haben Angreifer über eine Schwachstelle im Steuerungssystem tausende Autos stehlen können. Auch sie konnten die Fahrzeuge aufsperren und den Motor starten.

Bremsen ferngesteuert

Autodiebstähle wären aber noch das geringere Übel. Die Sicherheitsforscher Charlie Miller und Chris Valasek konnten vor einigen Jahren die Kontrolle über einen Jeep Cherokee übernehmen. Dies gelang ihnen über eine Schwachstelle im Infotainmentsystem. Über das Internet konnten sie das Fahrzeug fernsteuern und Hupe, Radio, Bremsen, Geschwindigkeit, Klimaanlage sowie Scheibenwischer kontrollieren. In einem Versuch verlor der Fahrer zunehmend die Kontrolle über den Wagen, der letztendlich in einen Graben rollte.

Fiat Chrysler ließ daraufhin 1,4 Millionen Fahrzeuge zurückholen – mit dem Update wurden derartige Angriffe aus der Ferne unmöglich gemacht.


Viel Elektronik im Auto bedeutet viele mögliche Schwachstellen


AIT PEM VIDRATZKY
Threatget zeigt potenzielle Gefahren und mögliche Lösungen auf